McGrathNicol

Where to start if you experience a data breach?

Spotlight shines again on information privacy

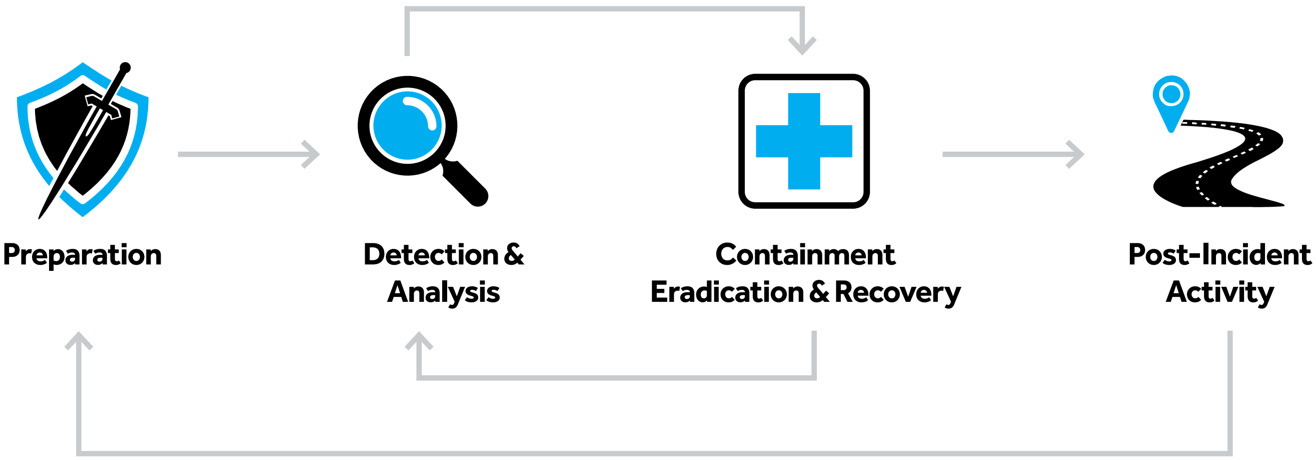
What is being called the largest data breach since the introduction of the Notifiable Data Breaches scheme has this week shone the spotlight again on risks associated with the security of private information and how this may affect every organisation, large or small. This week HR firm PageUp confirmed they had experienced a data breach. PageUp has over two million users across almost 200 different countries which include some of Australia's largest companies including Coles, Telstra, Wesfarmers and the CBA. Customers of PageUp are being asked to alert their users to the fact that job applicants using the service may have had their private information stolen. According to PageUp and its CEO, the breach initially occurred on May 23 however it wasn't until May 28 that their investigation determined data may have been compromised.

Understandably, customers of PageUp have been vocal about the lack of timely disclosure and the delays in notifying those affected, with many finding out about the breach through the press. As a result, some customers have now indicated they are considering legal action and notably, law firm Centennial Lawyers has stated that it is exploring a class action in relation to the breach.

Timely reminder for businesses

This is a timely reminder for businesses on the risks and responsibilities associated with protecting customer information. Reading about one's personal information having been compromised or stolen via the media is a strong indication that the process to identify, report and manage the breach has gone wrong and will almost certainly impact reputation and customer faith in the brand. Indeed, press articles about breaches are becoming far too common. Customers who entrust their personal particulars to a corporate entity or government agency have a right to expect security of their data or, at the very least, timely notification and response should a breach occur. Unfortunately the regularity of breaches means that people now may almost expect their information to be lost, stolen or compromised at some stage. Whilst many organisations are properly prepared and have a data breach plan ready to execute, many believe that their disaster recovery (DR) and business continuity plans (BCP) will suffice. That approach assumes a data breach will occur and as we now know, good incident response starts well before a breach is identified. Incident response preparation and in particular the post-incident activities that seek to understand and remediate the mistakes of the past, all play an important role in helping to protect the organisation and its customer information in the future.

Data Breach and Incident Response Framework



Preparation	Detection & Analysis	Containment, Eradication & Recovery	Post-Incident Activity
· Preparing to handle incidents · Proactive prevention of incidents	· Understanding attack vectors · Signs of an incident · Sources of precursors and indicators · Incident analysis · Incidet documentation · Incident prioritisation · Incident notification	· Choosing a containment strategy · Evidence gathering and handling · Identifying and attacking hosts · Eradication and recovery	· Lessons learned · Using collected incident data (intel) · Evidence retention

OAIC's suggested response for victims of a data breach

If you or your organisation has been the victim of a data breach the Office of the Australian Information Commissioner (OAIC) suggests you should first contact the organisation who suffered the breach seeking information. If you are not satisfied with the response you receive, you can contact the OAIC directly with your concerns. Information relating to the steps you can take if the following data breaches occur can be found **here**.

Possible data breaches

Financial information

e.g. credit card details, online banking login

Contact information

e.g. home address, email, phone number

Health information

Sensitive information

About sexuality, race, political views, etc.

Tax file number information

Government identity document information

e.g. driver's licence, Medicare card, passport